UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/918,062	07/30/2001	Keith Alexander Harrison	30006786-2	2570

7590 04/29/2008

HEWLETT-PACKARD COMPANY
Intellectual Property Administration
P.O. Box 272400
Fort Collins, CO 80527-2400

EXAMINER	
DAVIS, ZACHARY A	
ART UNIT	PAPER NUMBER
2137	

MAIL DATE	DELIVERY MODE
04/29/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

Application Number: 09/918,062
Filing Date: July 30, 2001
Appellant(s): HARRISON ET AL.

Charles W. Griggers
(Reg. No. 47,283)
For Appellant

EXAMINER'S ANSWER

This is in response to the appeal brief filed 07 February 2008 appealing from the Office action mailed 24 May 2007.

(1) Real Party in Interest

A statement identifying by name the real party in interest is contained in the brief.

(2) Related Appeals and Interferences

The following are the related appeals, interferences, and judicial proceedings known to the examiner which may be related to, directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal:

Application Serial No. 09/918,326 (Appeal No. 2007-3443) is a related application. Subsequent to the filing of Appellant's Brief in the present application, a decision was mailed in the above related application affirming the Examiner's rejections, a copy of which is provided.

(3) Status of Claims

The statement of the status of claims contained in the brief is correct.

(4) Status of Amendments After Final

No amendment after final has been filed.

(5) Summary of Claimed Subject Matter

The summary of claimed subject matter contained in the brief is correct.

(6) Grounds of Rejection to be Reviewed on Appeal

The appellant's statement of the grounds of rejection to be reviewed on appeal is correct.

(7) Claims Appendix

The copy of the appealed claims contained in the Appendix to the brief is correct.

(8) Evidence Relied Upon

5,598,473	LINSKER et al	1-1997
6,862,583	MAZZAGATTE et al	3-2005

5,633,932	DAVIS et al	5-1997
5,448,045	CLARK	9-1995

Menezes et al. Handbook of Applied Cryptography. CRC Press, 1997. pp. 397-405

(9) Grounds of Rejection

The following ground(s) of rejection are applicable to the appealed claims:

Claim Rejections - 35 USC § 103

Claims 1-12 and 14-19 are rejected under 35 U.S.C. 103(a) as being unpatentable over Linsker et al, US Patent 5598473, in view of Mazzagatte et al, US Patent 6862583; Davis et al, US Patent 5633932; and Menezes et al, *Handbook of Applied Cryptography*.

In reference to **Claims 1, 5, and 8**, Linsker discloses a method for determining the authenticity of a fax document (column 2, lines 23-27) that includes receiving a document and a digest of the document created by a hash algorithm and encrypted with a first token of the sender, which is the sender's private key (column 4, lines 54-60, where digest signature DS is the encrypted digest); obtaining a second token of the sender, which is the sender's public key, relating to the private key (column 4, lines 57-65); decrypting the digest with the public key (column 5, lines 20-23); creating a second digest using a hash algorithm (column 5, lines 23-27, and column 4, lines 25-35); and comparing the decrypted received digest with the second created digest (column 5, lines 23-42). However, although Linsker discloses authenticating the sender of a document, Linsker does not explicitly disclose verifying the identity of the intended recipient of a document.

Mazzagatte discloses a method for authenticated secure printing, which can be implemented for fax documents (column 4, lines 35-37), and which includes receiving and securely retaining a digital document and a transmitted independently verifiable data record of an intended recipient at a printout station (column 8, line 20-column 9, line 7; noting column 8, line 63-column 9, line 1, where the data is securely stored at the printer; further noting column 8, lines 20-29, where the digital certificate is the independently verifiable data record); obtaining a first token of the intended recipient, which is the recipient's private key (column 4, lines 9-12); requesting proof of the intended recipient's identity at the printout station using the independently verifiable data record (column 9, lines 49-51); and releasing the document when the intended recipient's identity has been proven by use of the first token of the intended recipient that is related to a second token of the recipient, where the second token is the recipient's public key (column 9, lines 46-62). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the method of Linsker by including verification of the intended recipient in addition to authentication of the sender, in order to ensure that printout of sensitive documents is authorized and that print data is securely stored (see Mazzagatte, column 2, lines 7-10).

Although Linsker discloses authenticating the sender of a document and Mazzagatte discloses verifying the identity of the intended recipient of a document, neither Linsker nor Mazzagatte explicitly discloses that identification data is encrypted specifically by the transmission station. Davis discloses a method for user authentication at a print node, which may process fax documents (see column 1, lines 39-45), and which includes receiving and securely retaining a digital document and a transmitted independently verifiable data record of an intended recipient at a printout station (column 5, lines 13-24; column 6, lines 38-40); obtaining a first token of the intended recipient, which is the recipient's

private key (see column 5, lines 52-65); requesting proof of the intended recipient's identity at the printout station using the independently verifiable data record (column 5, lines 52-65; column 6, lines 40-41); decrypting identifying data with the first token (see column 5, lines 13-18 and 52-65), where the data was encrypted with the second token of the intended recipient, which is the recipient's public key, and the data was encrypted at the transmitting station (column 4, line 39-column 5, line 9, where a header is encrypted at the sending node, where the header can include information identifying the intended recipient); determining the authenticity of the recipient of the document (column 5, line 33-column 6, line 8, noting particularly column 5, lines 52-65 where a private key on a smart card and a challenge/response protocol are used for authentication); and releasing the document when the intended recipient's identity has been proven by use of the first token (column 5, lines 21-24; column 6, lines 41-45). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the method of Linsker and Mazzagatte by including encryption of identifying data at the transmitting station, in order to allow for confirmation that the intended recipient is present using authentication techniques (see Davis, column 2, lines 26-29, and column 4, lines 65-67).

Although Linsker, Mazzagatte, and Davis disclose that the independently verifiable data record includes identification data (Mazzagatte, column 8, lines 20-30) and that a challenge/response protocol is used to authenticate and prove the intended recipient's identity (Mazzagatte, column 9, lines 58-61; Davis, column 5, lines 58-65), Linsker, Mazzagatte, and Davis do not explicitly disclose that the challenge/response protocol decrypts encrypted identification data with the recipient's private key, where the identification data was encrypted with the recipient's public key. However, Menezes discloses that challenge-response identification and authentication can be performed based on

public-key decryption (page 403, Section 10.3.3, first paragraph). Menezes further discloses that the protocol includes encrypting a challenge, which can be an identifier, with a public key, decrypting the encrypted challenge with a private key to form the response, comparing the challenge and response, and verifying the identity if the comparison result indicates a match (page 404, "(i) Challenge-response based on public-key decryption", noting that, in addition to random numbers, identifier "B" is one of the parts of the challenge). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the method of Linsker, Mazzagatte, and Davis by implementing the challenge/response protocol in the manner suggested by Menezes, in order to identify the recipient based on its private key (page 403, Section 10.3.3, first paragraph) and avoid chosen text attacks (page 404, paragraph "Identification based on PK decryption and witness").

In reference to **Claims 2 and 3**, Linsker, Mazzagatte, Davis, and Menezes further disclose receiving a digital certificate of the sender and that the public key is part of the certificate (see Linsker, column 5, lines 2-13).

In reference to **Claim 4**, Linsker, Mazzagatte, Davis, and Menezes further disclose checking the validity of the certificate online (see Linsker, column 5, lines 6-13).

In reference to **Claims 6 and 7**, Linsker, Mazzagatte, Davis, and Menezes further disclose printing the document with a verifying mark once it has been authenticated (see Linsker, column 6, lines 3-29).

In reference to **Claims 9, 10, and 17**, Linsker discloses a method of sending a fax document (column 2, lines 23-27) that includes creating a digest of the document using a hash algorithm (column 4, lines 25-35); encrypting the digest with a first token of the sender, which is the sender's

private key (column 4, lines 40-47); obtaining a second token of the sender, specifically the sender's public key, that will be used to decrypt the encrypted digest; and sending the encrypted digest, the document, and the public key to the recipient (column 4, lines 50-53). However, although Linsker discloses authenticating the sender of a document, Linsker does not explicitly disclose verifying the identity of the intended recipient of a document.

Mazzagatte discloses a method for authenticated secure printing, which can be implemented for fax documents (column 4, lines 35-37), and which includes receiving and securely retaining a digital document and a transmitted independently verifiable data record of an intended recipient at a printout station (column 8, line 20-column 9, line 7; noting column 8, line 63-column 9, line 1, where the data is securely stored at the printer; further noting column 8, lines 20-29, where the digital certificate is the independently verifiable data record); requesting proof of the intended recipient's identity at the printout station using the independently verifiable data record (column 9, lines 49-51); and releasing the document when the intended recipient's identity has been proven by use of a second token of the intended recipient that is related to the recipient's first token, where the second token is the recipient's private key (column 9, lines 46-62). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the method of Linsker by including verification of the intended recipient in addition to authentication of the sender, in order to ensure that printout of sensitive documents is authorized and that print data is securely stored (see Mazzagatte, column 2, lines 7-10).

Although Linsker discloses authenticating the sender of a document and Mazzagatte discloses verifying the identity of the intended recipient of a document, neither Linsker nor Mazzagatte explicitly discloses that identification data is encrypted specifically by the transmission station. Davis discloses

a method for user authentication at a print node, which may process fax documents (see column 1, lines 39-45), and which includes obtaining a first token of the intended recipient, which is the recipient's public key (column 3, line 40-column 4, line 56); encrypting identification information of the intended recipient using the first token of the recipient (column 4, line 39-column 5, line 9, where a header is encrypted at the sending node, where the header can include information identifying the intended recipient); sending and then receiving and securely retaining a transmitted document, the encrypted identification information, and a transmitted independently verifiable data record of an intended recipient at a printout station (column 5, lines 13-24; column 6, lines 38-40); requesting proof of the intended recipient's identity at the printout station using the independently verifiable data record (column 5, lines 52-65; column 6, lines 40-41); decrypting identifying data with a second token, which is the private key of the recipient (see column 5, lines 13-18 and 52-65); determining the authenticity of the recipient of the document (column 5, line 33-column 6, line 8, noting particularly column 5, lines 52-65 where a private key on a smart card and a challenge/response protocol are used for authentication); and releasing the document when the intended recipient's identity has been proven by use of the second token (column 5, lines 21-24; column 6, lines 41-45). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the method of Linsker and Mazzagatte by including encryption of identifying data at the transmitting station, in order to allow for confirmation that the intended recipient is present using authentication techniques (see Davis, column 2, lines 26-29, and column 4, lines 65-67).

Although Linsker, Mazzagatte, and Davis disclose that the independently verifiable data record includes identification data (Mazzagatte, column 8, lines 20-30) and that a challenge/response protocol is used to authenticate and prove the intended recipient's identity (Mazzagatte, column 9,

lines 58-61; Davis, column 5, lines 58-65), Linsker, Mazzagatte, and Davis do not explicitly disclose that the challenge/response protocol decrypts the encrypted identification data with the recipient's private key. However, Menezes discloses that challenge-response identification and authentication can be performed based on public-key decryption (page 403, Section 10.3.3, first paragraph). Menezes further discloses that the protocol includes encrypting a challenge, which can be an identifier, with a public key, decrypting the encrypted challenge with a private key to form the response, comparing the challenge and response, and verifying the identity if the comparison result indicates a match (page 404, "(i) Challenge-response based on public-key decryption", noting that, in addition to random numbers, identifier "B" is one of the parts of the challenge). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the method of Linsker, Mazzagatte, and Davis by implementing the challenge/response protocol in the manner suggested by Menezes, in order to identify the recipient based on its private key (page 403, Section 10.3.3, first paragraph) and avoid chosen text attacks (page 404, paragraph "Identification based on PK decryption and witness").

In reference to **Claims 11 and 12**, Linsker, Mazzagatte, Davis, and Menezes further disclose proving the sender's identity by transferring data from a personal portable data carrier holding the private key to the transmission station from which the document will be sent, and that the sender enters a verifiable security identifier to establish the sender's identity (see Linsker, column 7, lines 13-21).

In reference to **Claims 14-16**, Linsker, Mazzagatte, Davis, and Menezes further disclose obtaining details of the sender, including the public key, from a central database, and providing the details and public key in a digital certificate (see Linsker, column 4, lines 50-53; column 5, lines 2-13).

Claims 18 and 19 are apparatus claims corresponding substantially to the methods of Claims 1 and 9, and are rejected by a similar rationale.

Claim 13 is rejected under 35 U.S.C. 103(a) as being unpatentable over Linsker in view of Mazzagatte, Davis, and Menezes as applied to claim 11 above, and further in view of Clark, US Patent 5448045.

Linsker, Mazzagatte, Davis, and Menezes disclose everything as applied above in reference to Claim 11. However, Linsker, Mazzagatte, Davis, and Menezes do not explicitly disclose that the digest is encrypted within the personal portable data carrier. Clark discloses that digital signatures (formed by encrypting a message digest with a private key) can be performed in smart cards (column 8, lines 53-58). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the method of Linsker, Mazzagatte, Davis, and Menezes to include encrypting the digest within the personal portable data carrier, in order to prevent compromise of the sender's private key (see Clark, column 8, lines 57-62).

(10) Response to Argument

A. The *Linsker* Reference

B. The *Mazzagatte* Reference

C. The *Davis* Reference

D. The *Menezes* Reference

Under the above four headings, Appellant purports to provide a summary of each of the noted references (pages 10-11 of the present Appeal Brief). The Examiner respectfully but emphatically disagrees with the description of the Menezes reference (see page 11 of the present Appeal Brief).

In particular, in contrast to Appellant's assertion, the cited portion of Menezes clearly does disclose using a token of an intended recipient to encrypt information that is transmitted by a sender to the recipient (see page 404, "(i) Challenge-response based on public-key decryption", where, in the first message labeled (1), the sender B sends to the intended recipient A information that has been encrypted using a token of the intended recipient, where $P_A(r, B)$ indicates encryption using the public key, i.e. token, of A, i.e. the intended recipient). The Examiner does not dispute any of the other characterizations of the remaining references. The issue of what is disclosed, taught, and/or suggested by the references in relation to the claim language is addressed in further detail in the statement of the grounds of rejection above and the further arguments below.

Prior to addressing the Appellant's further arguments, the Examiner notes, regarding the above references, that, as set forth above in the explanations of the grounds of rejection, the Linsker reference was largely relied upon for teachings of the claimed features regarding verification of an unknown sender of a document and of the document itself, whereas the Mazzagatte reference was relied upon for the broad teachings of the claimed features regarding verification of the intended recipient of a document. The Davis and Menezes references were further relied upon for providing more specific details of the features directed to verification of the intended recipient.

E. Rejection of Claims 1-12 and 14-19 under 35 U.S.C. 103(a) as unpatentable over Linsker in view of Mazzagatte, Davis, and Menezes.

1. Claim 1

In reference to independent Claim 1, in response to Appellant's arguments against the references individually, one cannot show nonobviousness by attacking references individually where

the rejections are based on combinations of references. See *In re Keller*, 642 F.2d 413, 208 USPQ 871 (CCPA 1981); *In re Merck & Co.,* 800 F.2d 1091, 231 USPQ 375 (Fed. Cir. 1986). In particular, Appellant separately argues that none of the Linsker, Mazzagatte, Davis, and Menezes references individually discloses identification information from an independently verifiable data record that is encrypted using a second token of the recipient by a transmitting station (see pages 13-15 of the present Appeal Brief). The Examiner notes that these arguments are repeated nearly verbatim from Appellant's response received 08 March 2007, and these arguments were previously addressed in the final Office action mailed 24 May 2007. The Examiner's responses and clarifications thereto are provided hereinbelow for convenience.

Appellant argues that Mazzagatte does not teach or suggest information being encrypted using a token (i.e. public key) of an intended recipient and then transmitted (see pages 13 of the present Appeal Brief). The Examiner notes that Mazzagatte was not explicitly relied upon for teaching this specific feature. Rather, Mazzagatte was relied upon for more general teachings of verifying the intended recipient of a document, as noted above (see, for example, column 8, line 20-column 9, line 7; noting column 8, line 63-column 9, line 1, where a document is securely stored at the printer; column 9, lines 46-62, where the document is released when the intended recipient's identity has been verified by use of the intended recipient's public/private key pair).

Appellant also argues that Linsker does not "remedy the deficiencies of Mazzagate [sic]" and "does not teach or suggest that information is encrypted using a token of an intended recipient" but only "teaches that information is encrypted using a token of a sender" (pages 13-14 of the present Appeal Brief, emphasis appellant's). First, the Examiner notes that encryption of information using a token of a sender is also recited in Claim 1 (see the limitation beginning "receiving and securely

retaining…" where a digest is encrypted using a token of a sender, quoted and emphasized at page 12 of the present Appeal Brief, for example), and Linsker was specifically relied upon for a teaching of such a limitation, which Appellant has not disputed. Further, the Examiner again notes that Linsker was not explicitly relied upon for a teaching of encryption using a token of an intended recipient. Rather, Linsker was relied upon for teachings of the claimed features related to the verification of an unknown sender of a document and/or of that document itself, which is claimed as the intended use of the method of Claim 1, and, indeed, each of the independent claims (see the preamble of present Claim 1; see also the preambles of independent Claims 9, 18, and 19). In contrast, the remaining references (Mazzagatte, Davis, and Menezes) were relied upon for teachings of the other claimed features directed to the verification of the intended recipient of the document, as noted above. Additionally, as an aside, the Appellant is reminded that the primary reference relied upon in the above rejection was Linsker, and not Mazzagatte (noting the order in which the references were addressed suggests that Mazzagatte may have been considered by the Appellant to be the primary reference relied upon, see pages 13-14 of the present Appeal Brief).

Appellant further argues that Menezes does not teach or suggest using a token of an intended recipient to encrypt information transmitted by a sender to the recipient (page 14 of the present Appeal Brief). As noted above, the Examiner respectfully but emphatically disagrees, noting that the cited portion of Menezes clearly does disclose using a token of an intended recipient to encrypt information that is transmitted by a sender to the recipient (see page 404, "(i) Challenge-response based on public-key decryption", where, in the first message labeled (1), the sender B sends to the intended recipient A information that has been encrypted using a token of the intended recipient, where $P_A(r, B)$ indicates encryption using the public key, i.e. token, of A, i.e. the intended recipient).

Appellant additionally argues that although Davis discloses encrypting identifying information using a public key of a printing node, Davis does not disclose encrypting the information using the public key of an intended recipient, drawing a distinction between the public key (i.e. claimed token) of the targeted printing node in contrast with the public key of the intended recipient (e.g. the user of the printing node; see page 14 of the present Appeal Brief). However, the Examiner did not previously dispute that characterization of Davis and previously noted in the statement of rejection that Linsker, Mazzagatte, and Davis "do not explicitly disclose that the challenge/response protocol decrypts encrypted identification data with the recipient's private key, where the identification data was encrypted with the recipient's public key" (see above); instead, Menezes was relied upon for a teaching of such a limitation as set forth in the previous Office action (see also above in the explanations of the grounds of rejection).

Therefore, the Examiner respectfully disagrees and submits that, at least in combination, Menezes and Davis at the very least suggest encrypting identifying information with the public key of the intended recipient and transmitting that information from the sender. Specifically, in view of Davis' teaching that at least the public key of the intended recipient, to be used for authentication of the intended recipient, is transmitted from the sender to the receiver (column 4, line 62-column 5, line 1) and that a challenge response protocol can be used for that authentication using the public key of the intended recipient (column 5, lines 52-65) and further in view of Menezes' disclosure of encrypting identification information using the public key of the intended recipient (page 404, "(i) Challenge-response based on public-key decryption", where P_A denotes encryption using the public key of the recipient, and where an identifier is also included in the encryption, as cited above), the combination of at least Menezes and Davis clearly discloses that the identification information is encrypted by the

public key of the intended recipient (again, see Menezes, page 404) and at least fairly suggests that such encryption would take place at the sender before the document as a whole would be sent (noting in particular the disclosure in Davis of the document and the control information of the header being encrypted at the sender, column 4, line 39-column 5, line 9).

In response to the above argument, Appellant "notes that Davis and Menezes disclose a type of authentication of executing a challenge/response protocol with a public token of an intended recipient. Neither Davis nor Menezes discloses using a token of an intended recipient to encrypt information that is transmitted by a sender to the recipient" (page 15 of the present Appeal Brief). The Examiner once again respectfully but emphatically disagrees, again noting that Menezes clearly discloses using a token of an intended recipient to encrypt information that is transmitted by a sender to the recipient (see page 404, cited above). Also in response to the above argument, Appellant "notes that this portion of the Davis reference refers to encryption using a public key of a printing node and not that of an intended recipient" (page 15 of the present Appeal Brief, referring to column 4, line 39-column 5, line 9 of Davis). In response, the Examiner again notes that the Menezes reference, and not the Davis reference, was relied upon for the specific detail of encryption using the public key of an intended recipient in contrast to the public key of the printing node (again, see Menezes, page 404, and the explanation of the grounds of rejection detailed above).

2. Claims 2-8

Appellant does not argue the merits of Claims 2-8 separately and only relies on their dependence on independent Claim 1, addressed above (see page 16 of the present Appeal Brief).

3. Claim 9

Although Appellant separately argues the rejection of independent Claim 9, the substance of the arguments corresponds substantially to that of the arguments addressed above in reference to the rejection of independent Claim 1 (see pages 17-19 of the present Appeal Brief, where Appellant again generally argues that none of the references individually teach or suggest encrypting identification data using a token of the intended recipient and more specifically argues that Menezes does not teach or suggest using a token of an intended recipient to encrypt information that is transmitted by a sender to the recipient).

4. Claims 10-12 and 14-17

Appellant does not argue the merits of Claims 10-12 or 14-17 separately and only relies on their dependence on independent Claim 9, addressed above (see page 19 of the present Appeal Brief).

5. Claim 18

6. Claim 19

Similarly to independent Claim 9, although Appellant separately argues the rejection of independent Claims 18 and 19, the substance of the arguments corresponds substantially to that of the arguments addressed above in reference to the rejection of independent Claim 1 (see pages 20-26 of the present Appeal Brief, where Appellant argues, *inter alia*, that Menezes does not teach or suggest using a token of an intended recipient to encrypt information that is transmitted by a sender to the recipient).

F. Rejection of Claim 13 under 35 U.S.C. 103(a) as unpatentable over Linsker in view of Mazzagatte, Davis, and Menezes, and further in view of Clark

Appellant does not argue the merits of Claim 13 separately and only relies on the dependence on independent Claim 9, addressed above (see page 27 of the present Appeal Brief).

(11) Related Proceeding(s) Appendix

Copies of the court or Board decision(s) identified in the Related Appeals and Interferences section of this examiner's answer are provided herein.

For the above reasons, it is believed that the rejections should be sustained.

Respectfully submitted,

Zachary A. Davis

/Zachary A Davis/
Examiner, Art Unit 2137

Conferees:

/KIMYEN VU/

Supervisory Patent Examiner, Art Unit 2135

/HOSUK SONG/

Primary Examiner, Art Unit 2135